

# Browsing Safely: Understanding Active Content and Cookies

## National Cyber Alert System - Cyber Security Tip ST04-012

Many people browse the Internet without much thought to what is happening behind the scenes. Active content and cookies are common elements that may pose hidden risks when viewed in a browser or email client.

### What is active content?

To increase functionality or add design embellishments, web sites often rely on scripts that execute programs within the web browser. This active content can be used to create "splash pages" or options like drop-down menus. Unfortunately, these scripts are often a way for attackers to download or execute malicious code on a user's computer.

- JavaScript - JavaScript is just one of many web scripts (other examples are VBScript, ECMAScript, and JScript) and is probably the most recognized. Used on almost every web site now, JavaScript and other scripts are popular because users expect the functionality and "look" that it provides, and it's easy to incorporate (many common software programs for building web sites have the capability to add JavaScript features with little effort or knowledge required of the user). However, because of these reasons, attackers can manipulate it to their own purposes. A popular type of attack that relies on JavaScript involves redirecting users from a legitimate web site to a malicious one that may download viruses or collect personal information.
- Java and ActiveX controls - Different from JavaScript, Java and ActiveX controls are actual programs that reside on your computer or can be downloaded over the network into your browser. If executed by attackers, untrustworthy ActiveX controls may be able to do anything on your computer that you can do (such as running spyware and collecting personal information, connecting to other computers, and potentially doing other damage). Java applets usually run in a more restricted environment, but if that environment isn't secure, then malicious Java applets may create opportunities for attack as well.



JavaScript and other forms of active content are not always dangerous, but they are common tools for attackers. You can prevent active content from running in most browsers, but realize that the added security may limit functionality and break features of some sites you visit. Before clicking on a link to a web site that you are not familiar with or do not trust, take the precaution of disabling active content.

These same risks may also apply to the email program you use. Many email clients use the same programs as web browsers to display HTML, so vulnerabilities that affect active content like JavaScript and ActiveX often apply to email. Viewing messages as plain text may resolve this problem.

## What are cookies?

When you browse the Internet, information about your computer may be collected and stored. This information might be general information about your computer (such as IP address, the domain you used to connect (e.g., .edu, .com, .net), and the type of browser you used). It might also be more specific information about your browsing habits (such as the last time you visited a particular web site or your personal preferences for viewing that site).

### Cookies can be saved for varying lengths of time:

-  Session cookies - Session cookies store information only as long as you're using the browser; once you close the browser, the information is erased. The primary purpose of session cookies is to help with navigation, such as by indicating whether or not you've already visited a particular page and retaining information about your preferences once you've visited a page.
-  Persistent cookies - Persistent cookies are stored on your computer so that your personal preferences can be retained. In most browsers, you can adjust the length of time that persistent cookies are stored. It is because of these cookies that your email address appears by default when you open your Yahoo! or Hotmail email account, or your personalized home page appears when you visit your favorite online merchant. If an attacker gains access to your computer, he or she may be able to gather personal information about you through these files.

To increase your level of security, consider adjusting your privacy and security settings to block or limit cookies in your web browser (see *Evaluating Your Web Browser's Security Settings* for more information). To make sure that other sites are not collecting personal information about you without your knowledge, choose to only allow cookies for the web site you are visiting; block or limit cookies from a third-party. If you are using a public computer, you should make sure that cookies are disabled to prevent other people from accessing or using your personal information.

Author: Mindi McDowell

Produced 2004 by US-CERT, a government organization.

Note: This tip was previously published and is being re-distributed to increase awareness.

Terms of use <http://www.us-cert.gov/legal.html>

This document can also be found at <http://www.us-cert.gov/cas/tips/ST04-012.html>.